Vol. 4, No. 2, Juni 2020, 143–152
E-ISSN: 2548-3412

# Implementasi dan Analisa Kinerja Jaringan *Wide Area Network* dengan *Open VPN-Access Server*

**Rian Septian Anwar[1], Nani Agustina[2*]**

[1] Ilmu Komputer; Universitas Bina Sarana Informatika; Jl. Kramat Raya No.98, Senen, Jakarta Pusat 10450, (021) 23231170/(021) 21236158; e-mail: rian.ptn@bsi.ac.id
[2] Sistem Informasi Akuntansi; Universitas Bina Sarana Informatika; Jl. Kamal Raya No. 18 Ringroad Barat, Cengkareng Jakarta Barat 11730, Indonesia, telp/fax (021) 54376398; e-mail: nani.nna@bsi.ac.id

* Korespondensi:e-mail: nani.nna@bsi.ac.id

Diterima: 18 Mei 2020; Review: 21 Mei 2020; Disetujui: 23 Mei 2020

Cara sitasi: Anwar RS, Agustina N. 2020. Implementasi dan Analisa Kinerja Jaringan *Wide Area Network* dengan *Open VPN-Access Server*. *Informatics for Educators and Professionals*. Vol 4 (2): 143-152.

---

**Abstrak**: Meningkatnya penggunaan internet di dunia, membuat trafik internet menjadi tinggi. Kebutuhan akan interkoneksi antar jaringan yang meningkat terutama pada perusahaan yang mempunyai banyak cabang. Oleh karena itu perusahaan dituntut untuk mengeluarkan budget lebih banyak lagi. Untuk meredam pengeluaran yang terlalu berlebih maka dibutuhkan dibutuhkan sebuah jaringan *Virtual Private Network* (VPN). Dengan memanfaatkan Open VPN-*Access Server* biaya yang dikeluarkan lebih murah dibandingkan dengan sewa VPN-IP yang relatif lebih mahal biayanya. Untuk jaringan yang lebih baik, maka harus ditopang dengan struktur topology terbaik menurut pemasangannya. Pemilihan topology pada awal pembangunan jaringan sangat penting untuk membuat akses *Virtual Private Network* (VPN) ini terkoneksi dengan baik.

**Kata kunci:** *Virtual Private Network*, Jaringan, Open VPN-Acces Server.

***Abstract:*** *The increasing use of the internet in the world, making internet traffic become high. The need for interconnection between networks is increasing in companies with many branches. Therefore companies are required to spend even more budget. To reduce excess expenditure, a Virtual Private Network (VPN) is needed. By utilizing Open VPN-Server Access that is issued is cheaper compared to VPN-IP leases that are relatively more expensive. For better tissue, it must be supported by the best topological structure according to installation. The choice of topology at the beginning of network development is very important to make this Virtual Private Network (VPN) access well connected.*

***Keywords****: Virtual Private Network, Networking, Open VPN-Acces Server.*

## 1. Pendahuluan

Perkembangan teknologi informasi mengalami peningkatan yang pesat dari tahun ke tahun. Teknologi informasi seperti jaringan komputer memberikan kemampuan sebagai media komunikasi yang dapat mempercepat proses kerja baik dari segi waktu maupun ruang [1]. Perkembangan teknologi jaringan lokal yang efisien dalam implementasi dan pengembangan jaringan komputer dapat meningkatkan mobilitas dan fleksibilitas *user*, dengan adanya teknologi *wireless* transaksi dapat dilakukan dimana saja selama masih dalam jangkauan. Selain itu, teknologi informasi dapat mempermudah dalam mengakses sebuah informasi. Sehingga perkembangan teknologi informasi sangat berpengaruh dalam segala kehidupan manusia [2].

Internet merupakan komponen penting dalam perkembangan teknologi saat ini. Bahkan internet sudah menjadi kebutuhan primer dalam sebuah lembaga atau organisasi. Kehadiran internet dapat mempermudah manusia untuk berkomunikasi dan berkoordinasi dengan yang

lainnya. Keterbukaan dalam akses internet dapat dilakukan semua kalangan dengan kondisi keterbukaan akses internet akan memungkinkan terjadinya pengaksesan data oleh pihak yang tidak berwenang misalnya pencurian data, penyadapan bahkan sampai level peretasan komputer maupun server [3].

Jaringan nirkabel menjadi target yang sangat menarik untuk para hacker. Pernyataan ini menidentifiksikan bahwa semua aspek selalu beresiko, ada aspek yang baik dan buruk yang akan selalu mengikuti. Dan yang paling utama dan menarik adalah dari sisi keamaan dalam hal sosialisasi manusia, interaksi dan komunikasi [4].

Perkembangan yang begitu pesat dan popular menjadikan pihak yang tidak bertanggungjawab mencari celah-celah untuk dapat memanfaatkannya secara ilegal dan tidak bermaksud bagi kebaikan. Bukan mustahil bahwa saat ini jaringan *wireless* menjadi target utama bagi para *hacker*. Beberapa organisasi dan perusahaan semakin gencar mengembangkan jaringan *wireless* karena kemudahan, kenyamanan, dan harga peralatan yang semakin terjangkau. Di pasaran, peralatan-peralatan *wireless* ini secara default tidak mempunyai fitur keamanan yang memadai, sehingga keberadaan peralatan *wireless* menjadi target utama para hacker untuk mencoba memanfaatkan berbagai kelemahannya. Hal ini didukung lagi dengan dokumen-dokumen peralatan wireless yang dengan mudah diperoleh di website secara bebas, baik dari segi teknis detail hingga operasionalnya. Banyak teknologi *software* dan *hardware* yang bisa dipakai untuk mengembangkan VPN ini. Dari teknologi yang *opensource* sampai yang berbayar dengan masing-masing kelebihannya dan kekurangnya dapat dengan mudah kita temukan [5].

*Virtual Private Network* (VPN) hubungan antar jaringan komputer satu dengan jaringan komputer lainnya secara private melalui jaringan internet atau dapat juga sebagai pelantara antar jaringan yang bersifat private, karena hanya orang tertentu yang dapat mengakses jaringan tersebut [6].

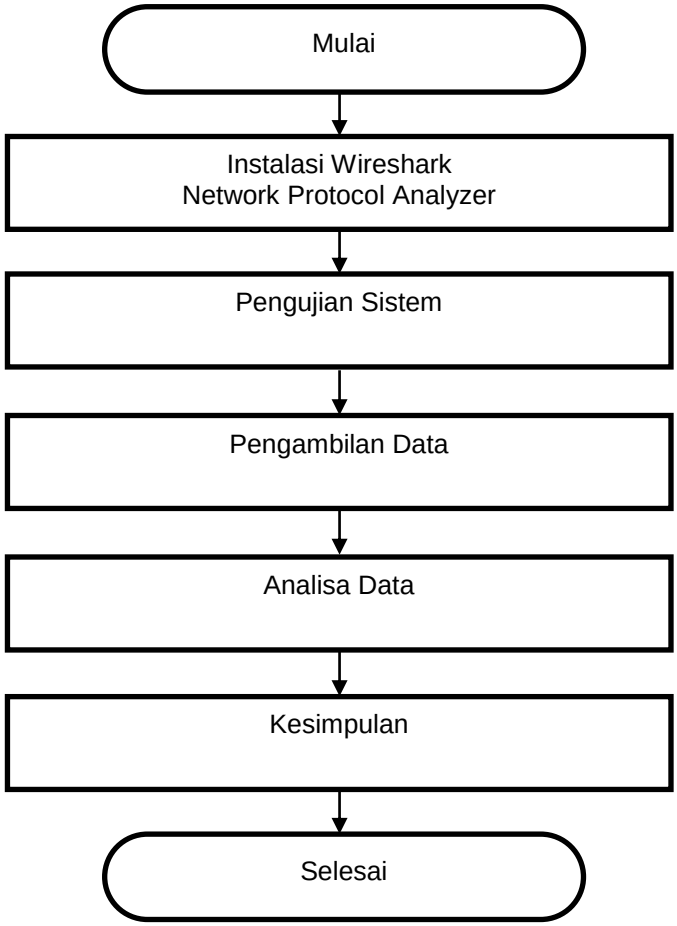
Pada penulisan membahas penggunaan aplikasi penunjang dalam pembuatan VPN yang bersifat *opensource*. Aplikasi penunjang tersebut yaitu *OpenVPN Access Server*. Penulis memilih *OpenVPN Access Server* karena memiliki semua fitur keamanan *OpenVPN, OpenVPN* menggunakan *private keys, certificate*, atau *username-password* untuk melakukan autentikasi dalam membangun koneksi, dimana untuk enkripsi *OpenVPN* sendiri menggunakan SSL/TLS yang dimana pembuatan *certificate* SSL-nya dilakukan oleh *OpenSSL* yang telah disediakan oleh Linux. Dalam implementasi dan penggunaanya relatif mudah karena sudah menggunakan *Grapical User Interface(GUI)* berbasis WEB.

## 2. Metode Penelitian

Metodologi penelitian yang digunakan meliputi Analisa Penelitian dan Metode Pengumpulan Data. Analisa penelitan yang digunakan penulis terdiri dari analisa kebutuhan, desain, testing dan implementasi berikut penjelasannya:1.Bahan Penelitian dengan menentukan materi yang ada pada penelitian keamanan jaringan *virtual private network* (VPN) dengan melihat yang sudah diterapkan sebelumnya. 2. Menentukan alat penelitian dengan menggunakan komputer dengan spesifikasi yang layak untuk menjalankan sofware aplikasi *virtual private network* (VPN). 3. Metode Penelitian dengan melakukan survey ke lokasi penelitan dengan datang dan melakukan survey ke lokasi penelitian untuk mengumpulkan study pustaka dan analisis data dengan melakukan penelitian terhadap analisa kebutuhan melakukan observasi dan wawancara untuk mengetahui kebutuhan dan permasalahan yang ada pada jaringan perusahaan. Tahapan kedua membuat desain jaringan VPN yang akan di implementasikan. Langkah ketiga melakukan testing meliputi tes koneksi dan juga tes keamanan untuk memastikan semuanya agar jaringan VPN sesuai yang diharapkan sebelum diimplementasikan. Pada tahapan ke empat Implementasi dengan menggunaan jaringan virtual mengunakan software VMWare versi 7.0.0 build-203739. Langkah yang dilakukan terakhir adalah Studi Pustaka dengan mendapatkan data-data secara teoritis sebagai bahan penunjang dalam mempelajari, meneliti dan menelaah berbagai literatur-literatur dari perpustakaan maupun dari buku-buku referensinya lainnya, juga dari situs-situs internet yang berkaitan dengan topik penelitian.

Penelitian akan dilakukan melalui dua tahap, yaitu pertama, menguji sistem yang tidak menggunakan VPN dan kedua, menguji sistem yang menggunakan VPN.

E-ISSN: 2548-3412; 143-152




Sumber: Hasil Penelitian (2020)

Gambar 1. Tahapan dalam Metode Penelitian

## 3. Hasil dan Pembahasan

### 3.1. Topologi Jaringan

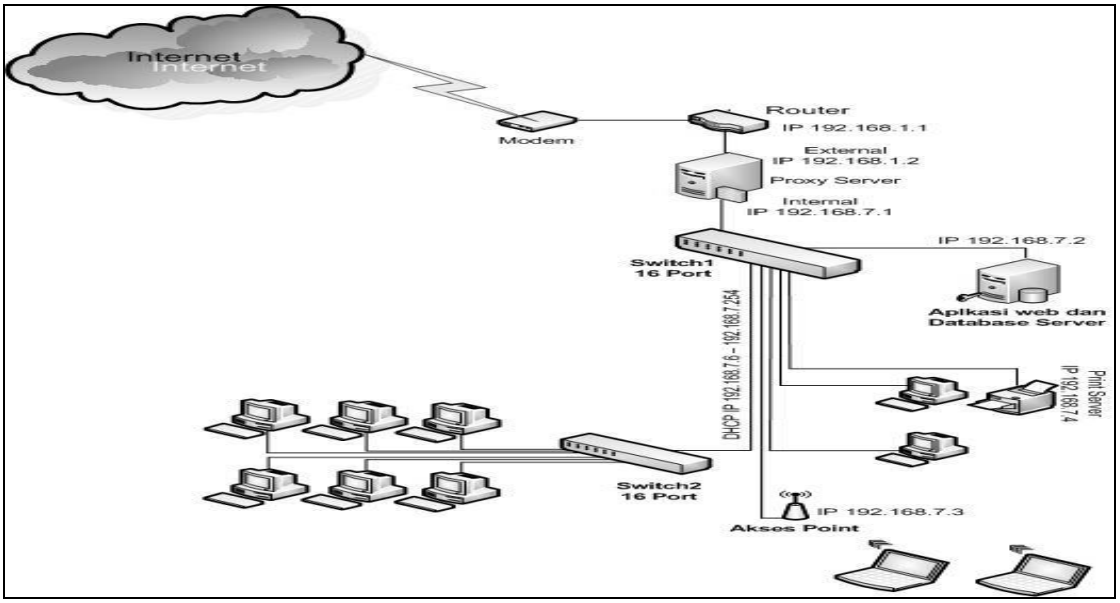
Topologi jaringan merupakan hal yang paling mendasar dalam membentuk sebuah jaringan yaitu *Topologi Tree*, dimana semua peralatan jaringan seperti PC, *Server*, Printer dan lainnya dihubungkan dalam satu konsentrator dalam hal ini *Switch*, kemudian *switch* tersebut dihubungkan ke *switch* lainnya untuk membentuk jaringan yang lainnya. *Traffic* data mengalir dari node ke *central node* dan kembali lagi dan juga jika salah satu kabel *node* terputus yang lainnya tidak terganggu.

Salah satu aturan dalam menghubungkan komputer (node) satu dengan lainnya secara fisik dan saling berkaitan antara satu komponen dengan komponen lainnya melalui peralatan atau media jaringa seperti server, workstation, hub atau pemasangan kabel biasanya dikenal dengan topologi jaringan [7].

Topologi jaringan atau arsitektur jaringan mengambarkan perencanaan hubungan antar komputer dalam Local Area Network yang umumnya menggunakan kabel sebagai media transmisi dihubungkan dengan koneketor dan *ethernet card* dan perangkatpendukung lainnya. Topologi yang terdapat pada hubungan komputer pada jaringa local area misalnya topologi star, topologi rong, topologi daisy-Chain, topologi Tree dan topologi mesh.

### 3.2. Skema Jaringan

Jaringan komputer (*Computer Network*) terdiri dari himpunan *interkoneksi* sejumlah komputer *antonomous.* Kata “Antonomous” bahwa komputer memiliki kendali atas dirinya sendiri bukan merupakan bagian dari komputer lain [8].




Sumber: Hasil Penelitian (2020)

Gambar 2. Skema Jaringan

Jaringan Komputer pada Mediatron terdiri dari *Modem, Router, Proxy server*, Web dan database *server*, dua buah *switch*, akses *point* dan *client* (PC dan Laptop).

*Switch* digunakan untuk menghubungkan seluruh perangkat (PC, *Server*, Printer dan perangkat jaringan lainnnya). *Switch*1 digunakan untuk menghubungkan modem, *server* aplikasi web, *proxy server* dan juga sebagai link ke akses *point* dan link ke *switch*2, sedangkan *switch*2 digunakan untuk menghubungkan PC-PC yang menjadi *client* di jaringan mediatron. Meditron juga menggunakan akses *point* untuk menghubungkan perangkat jaringan melalui media *wireless* seperti laptop dan perlangkat *wireless* lainnya.

Untuk aksses internet menggunakan jasa ISP Speedy dari PT. Telkom dengan *bandwidth* sebesar 2Mbps yang dishare ke semua *client* di jaringan internal mediatron melalui *Proxy server*. Akses internet ini sangat vital peranannya kare na digunakan untuk komunikasi terutama dalam penggunakan *e-mail* dan *messenger*. *E-mail* gunakan untuk komunikasi dengan *client* yang bekerjasama dengan transaksi bisnis.

### 3.3. Keamanan Jaringan

*Proxy Server* pada Mediatron memegang peranan penting dalam pengelolaan jaringan karena seluruh pengaturan jaringan seperti *management bandwidth* dan juga sebagai *Internet gateway* dipercayakan pada *proxy server*. *Proxy server* adalah *server* yang diletakan antara suatu aplikasi *client* dan aplikasi *server* yang dihubungi keamanan jaringan dan juga pengaturan akses internet diatur semua di *proxy server*. *Proxy server* menggunakan *ClearOS* versi 5.2. Di *proxy server* juga terdapat *firewall* untuk keamanan jaringan. *Firewall* adalah alat untuk melindungi jarigan *private* dari jaringan publik (internet) [9]. *Firewall* melindungi jaringan *private* dengan cara mengendalikan aliran paket berdasarkan pada asal tujuan, *port*, dan informasi tipe paket yang terdapat pada masing-masing paket. *Firewall* berisi sederet daftar aturan yang digunakan untuk menentukan nasib pada paket yang datang atau pergi dari *firewall* menurut kriteria dan parameter tertentu. Untuk keamaan disisi *client* masing-masing *client* diinstall juga program antivirus. Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan dimanapun ia berada. Jika dalam kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke kompter anda, dengan firewall semua itu dapat diatasi dengan mudah [10].

### 3.4. Permasalahan Sistem Jaringan

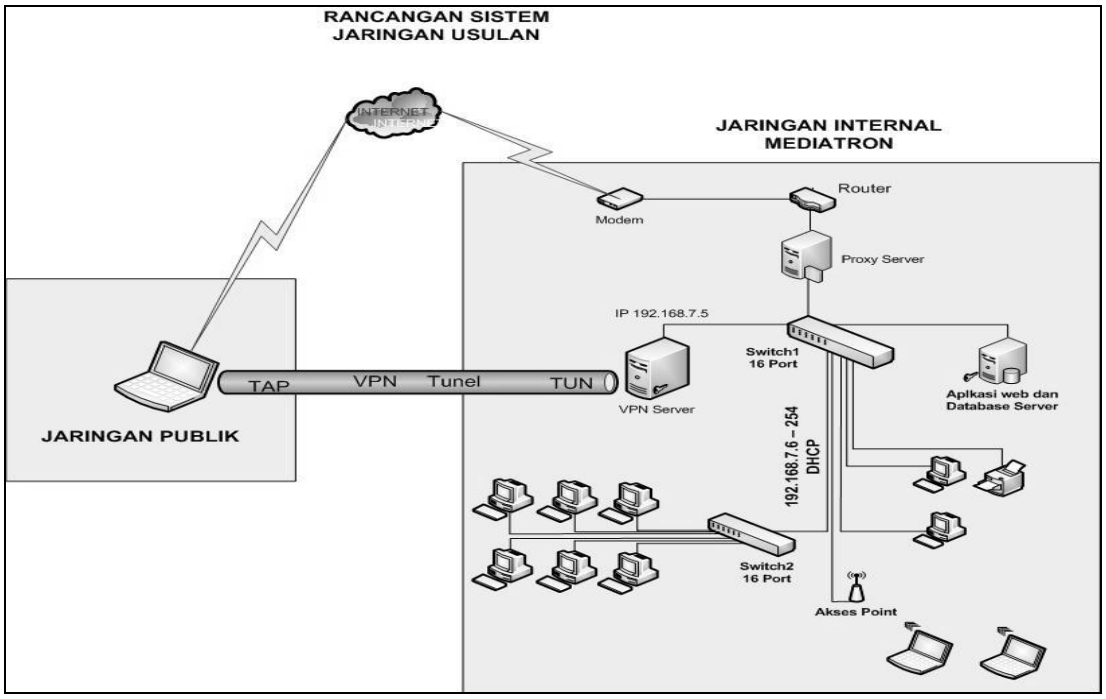
Permasalahan yang terjadi pada jaringan ini berdasarkan hasil pengamatan penulis biasanya para pengurus yang bekerja untuk mendapatkan data-data yang diperlukan sebagai

E-ISSN: 2548-3412; 143-152

bahan laporan dengan cara datang langsung ke kantor, cara ini sangat tidak efektif karena membutuhkan waktu dan tenaga yang tidak sedikit. Atau jika tidak ada waktu untuk datang ke kantor biasanya meminta bantuan staff administrasi untuk mengirim data yang diperlukan melalui *e-mail*, cara ini juga masih kurang efektif karena tidak ada sistem keamanan dalam pertukaran informasi, terlebih lagi *e-mail* yang digunakan masih menggunakan *e-mail free* dari layanan google yaitu gmail bukan dari *mail server* pribadi karena saat ini belum mempunyai *mail server* sendiri.

### 3.5. Alternatif Pemecahan Masalah

Untuk mengatasi masalah yang dialami, maka penulis mengusulkan untuk membangun jaringan *Virtual Private Network*, VPN dapat memberikan jaminan keamanan yang lebih baik dengan sistem autentikasi, hal ini dapat mencegah orang yang tidak berkepentingan untuk masuk ke dalam jaringan perusahaan. Aplikasi VPN yang penulis usulkan yaitu *OpenVPN Access Server* karena memiliki semua fitur keamanan yang ada pada *OpenVPN. OpenVPN* menggunakan *private keys, certificate,* atau *username-password* untuk melakukan autentikasi dalam membangun koneksi, dimana untuk enkripsi *OpenVPN* sendiri menggunakan SSL/TLS yang dimana pembuatan *certificate* SSL-nya dilakukan oleh *OpenSSL* yang telah disediakan oleh Linux*.* Dan juga dalam *OpenVPN Access Server* untuk implementasi dan penggunaanya relatif mudah karena sudah menggunakan *Grapical User Interface(GUI)* berbasis WEB. *OpenVPN Access Server* yang dalam penggunaan sangat *user friendly* baik disisi *server* karena sudah menggunakaan GUI *(graphical user interface)* berbasis Web dan disisi klien intalasi dan settingan dari *OpenVPN Access Server* relatif mudah.




Sumber: Hasil Penelitian (2020)

Gambar 3. Skema Jaringan Usulan

Pada Skema jaringan usulan dapat dilihat bahwa ada penambahan satu buah *server* VPN yang nantinya akan digunakan untuk bisa menghubungkan para pekerja yang berada di luar kantor ke jaringan LAN. Dikarenakan *VPN Server* ini dipasang di belakang *modem/router* dan *proxy server,* maka perlu dilakukan konfigurasi *port forward* disisi *modem/router* dan juga *proxy server*.

Dalam melakukan transfer data dengan jaringan VPN, data dienkripsi dan dienkapsulasi sehingga keamanan data terjaga. Data yang ditransfer dilewatkan dalam sebuah tunnel sehingga seolah-olah memiliki saluran jaringan sendiri yang pada kenyataannya transfer data menggunakan jaringan internet atau jaringan publik .

Dengan menerapkan Jaringan VPN dengan *OpenVPN,* maka pertukaran data melalui jaringan publik seperti internet akan terjamin keamannnya, ini dikarenakan ada sistem enkripsi data dan juga menggunakan teknologi *tunneling* antara VPN *client* dengan VPN *server*. Dan dalam penerapannya *tunnel* dilengkapi dengan sistem enkripsi untuk menjaga keamanan tersebut. Dimana data yang telah dienkripsi hanya dapat dibaca setelah didekripsi oleh *VPN server* atau *client* itu sendiri. *OpenVPN* standarnya menggunakan BF-CBC (*Blowfish-Cipher Block Chaining*) untuk Simetrik *cipher* menggunakan kunci 128-bit. Blowfish merupakan algoritma yang sangat kuat dan belum diketahui kelemahannya. kunci 128-bit memberikan kunci ruang yang cukup besar yang mustahil untuk melakukan serangan *brute force*. Blowfish tidak hanya sangat aman, tapi juga salah satu algoritma yang tercepat. Untuk memastikan integritas data *OpenVPN* menggunakan apa yang disebut *hash*, *hash* berfungsi menerima masukan *string* yang panjangnya sembarang lalu mentransformasikannya menjadi *string* keluaran yang panjangnya tetap (*fixed*). Fungsi *hash* sangat peka terhadap perubahan 1 bit pada pesan, Pesan berubah 1 bit, nilai *hash* berubah sangat signifikan. *OpenVPN* secara *default* menggunakan algoritma hashing SHA-1. untuk menghentikan penyerang yang ingin menghapus *hash string, OpenVPN* menggunakan HMAC. Pada saat pesan dikirim sebelumnya HMAC memasang kunci rahasia. Kunci ini dilampirkan pada *hash* bersama dengan pesan yang dikirim. Ketika pesan telah diterima di ujung terowongan, penerima akan membukan pesan dan memastikan kunci rahasia terbawa bersama dengan pesan yang diterima. Jadi jika ada penyerang mengubah pesan dan membuat *hash* baru maka mereka (penyerang) tidak bisa membuat kunci rahasia dan penerima bisa mengetahui bahwa pesan tersebut sudah berubah.

*OpenVPN* menggunakan *driver universal* TUN/TAP. *Driver* ini merupakan sebuah *virtual network interface* yang membentuk sebuah *tunnel*, bisa dilihat pada gambar 3 *virtual network interface* TUN dibentuk disisi *Server VPN* dan *virtual network interface* TAP dibentuk disisi VPN *client*.

### 3.6. Pengujian Jaringan awal

Pada Pengujian jaringan awal penulis melakukan tes koneksi dari sisi klien ke *server* dan dari sisi klien ke klien dengan cara melakukan *ping* dan melakukan *traceroute* ke situs internet untuk memastikan *client* bisa terkoneksi dengan *internet*. Hasilnya bisa dilihat pada gambar 4. Terlihat pada percobaan tersebut komputer *client* dapat terkoneksi dengan *server*, *client* lain dan internet dengan baik.

```
C:\Documents and Settings\user1>tracert google.co.id

Tracing route to google.co.id [173.194.38.183]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.7.1
  2     1 ms     1 ms     1 ms  192.168.1.1
  3    18 ms    19 ms    20 ms  180.242.228.1
  4    19 ms    19 ms    18 ms  193.subnet125-160-11.speedy.telkom.net.id [125.1
60.11.193]
  5    19 ms    19 ms    19 ms  61.94.114.105
  6    43 ms    39 ms    41 ms  226.128.240.180.telin.sg [180.240.128.226]
  7    52 ms    38 ms    39 ms  225.128.240.180.telin.sg [180.240.128.225]
  8   105 ms    39 ms    39 ms  72.14.211.61
  9   180 ms    40 ms    39 ms  209.85.243.156
 10   318 ms    41 ms    40 ms  72.14.233.105
 11    42 ms    41 ms    40 ms  sin04s02-in-f23.1e100.net [173.194.38.183]

Trace complete.
```

Sumber: Hasil Penelitian (2020)

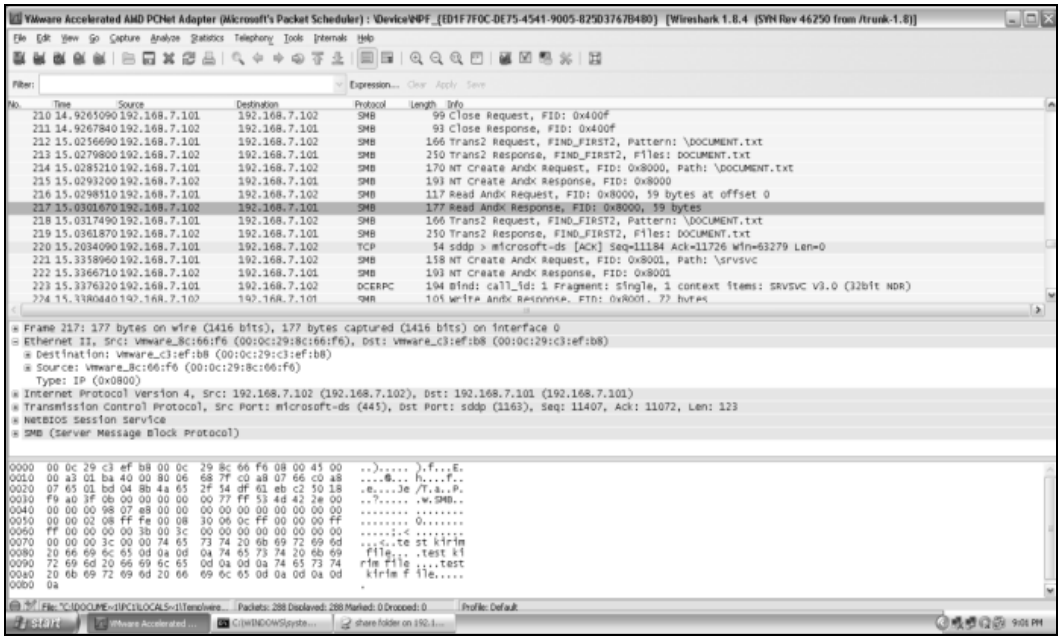
Gambar 4. Traceroute ke google.co.id

Pada pengujian awal keamanan data, penulis mencoba untuk *transfer file* dengan cara mengakses file DOCUMMENT.txt yang dishare pada PC *client* dengan IP *address* 192.168.7.102 bisa dilihat pada gambar 6. Kemudian proses tersebut di *capture* menggunakan *software wireshark* untuk menguji keamanannya.[11]

Dari hasil *capture* menggunakan *Whireshark*, nama file dan isi file dapat terbaca saat melakuakan *trasfer file* antra *client* yang menggunakan IP 192.168.7.102 dan *client* dengan IP

E-ISSN: 2548-3412; 143-152

192.168.7.10 menggunakan protokol Samba, File tersebut belum ter-enkripsi karena belum menggunakan VPN dan masih berada dalam jaringan internal dan belum memerlukan enkripsi data hasil percobaan tersebut bisa dilihat pada gambar 5.



Sumber: Hasil Penelitian (2020)

Gambar 5. Capture Wireshark File DOCUMENT.txt

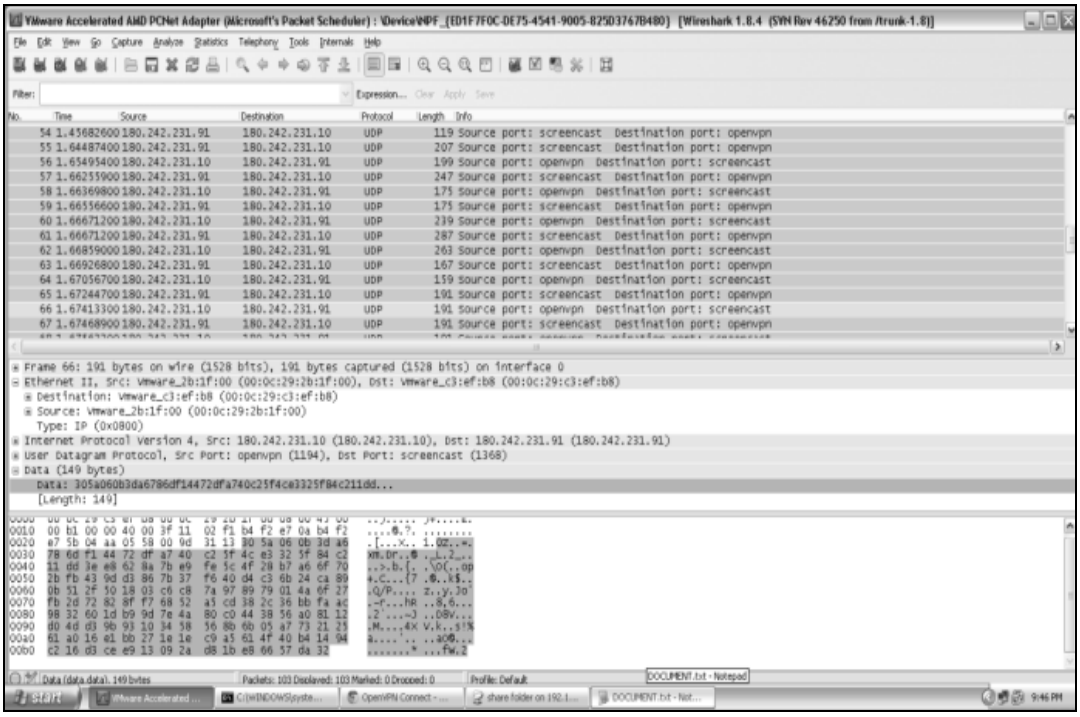
### 3.7. Pengujian Jaringan akhir

Selanjutnya pengujian jaringan setelah diimplementasikan VPN dengan uji koneksi dari *Remote Client* ke jaringan internal PT. Mediatron. Pada tahap uji koneksi setelah menggunakan VPN penulis akan mencoba koneksi menggunakan jaringan internal telkom karena yang akan menggunakan layanan VPN ini adalah pegawai telkom yang mempunyai jabatan sebagai pengurus. Pada percobaan awal penulis melakukan *ping* ke jaringan internet dalam hal ini penulis coba koneksi ke *website* google.com untuk memastikan jaringan lokal bisa terhubung ke internet dilanjutkan dengan melakukan uji koneksi ke VPN *server*.

Selanjutnya diteruskan dengan melakukan percobaan koneksi ke *VPN server* dengan cara buka *browser* kemudian di *address bar* ketikkan alamat IP publik VPN server yaitu : https://180.xxx.xxx.xx/ (ip publik disamarkan untuk menjaga privasi perusahaan) jika berhasil akan tampil pada browser kesalahan SSL atau sertifkat tidak, ini wajar karena sertifikat yang di buat ditandatangani sendiri oleh *server VPN* (*self-sign*). Jika tidak ingin mendapatkan tampilan seperti itu kita harus membeli sertifikat yang sudah ditandatangani oleh lembaga pembuat sertifikat, namun harganya tidak murah biasanya digunakan untuk web *e-bangking* dan *e-commerce* yang memang memerlukan keamanan dan kepercayaan dari penggunanya. Karena VPN ini digunakan hanya untuk keperluan internal perusahaan saja maka tidak diperlukan membeli sertifkat dari lembaga pembuat sertifikat seperti ***digicert*** atau ***symantec*** karena harganya yang cukup mahal. Berikut adalah tampilan login untuk koneksi ke *VPN server*.

Isikan *username* dan *password* kemudiaan pilih *connect* dan *go*. Sebelum koneksi, *client* perlu menginstall program untuk mengkonfigurasi *OpenVPN* secara otomatis file *instaler* bisa di *download* setelah *client* melakukan *authentikasi username* dan *password*. Setelah *download* selesai, klik dua kali file instalernya maka *OpenVPN* klien akan terkonfigurasi secara otomatis.

Dalam uji keamanan penulis coba akses ke *folder sharing* yang ada di PC dengan IP 192.168.7.102 dan mencoba untuk mengambil data yang ada di *folder sharing*, isi dari *folder sharing* nama file DOCUMENT.txt. Dalam proses pengambilan *file* yang ada di *folder share* pada jaringan internal mediatron penulis melakukan *sniffing* menggunakan software *wireshark* hasilnya bisa dilhat pada gambar 6.



Sumber: Hasil Penelitian (2020)

Gambar 6. *Capture Whireshark* Setelah menggunakan VPN

Bisa dilihat pada gambar 6 proses *trasfer file* baik nama file yang di *transfer* maupun isi dari *file* tidak terbaca oleh *wireshark* dan IP *address* yang ada di jaringan internal mediatron juga tidak terlihat, jadi terbukti bahwa dengan *OpenVPN* jaringan lokal dan data yang ada di Perusahaan terlidungi dengan aman.

Open VPN dapat menjadi pilihan terbaik untuk membuat interkoneksi antar perusahan dengan biaya lebih hemat dan data tetap aman. Pengujian menggunakan wheresark ini sangat teruji, karena sudah dilakukan penelitian akan software tersebut. namun keakuratan belum tentu 100% aman, bisa saja jika dikemudian hari kemajuan teknologi yang semakin berkembang, membuat aplikasi ini mempunya celah atau kebocoran port sehingga data menjadi tidak aman. Dalam pengujian latency dengan Open VPN dilakukan dengan kombinasi dan otentifikasi pada lima kali periode pengiriman data icmp sebesar 100, 200, 500, 1000 dan 1500 byte dengan pengulangan 100 kali persatukali periode dan pada waktu yang berbeda untuk kombinasi dan otentikasi. Berikut ini tabel rincian pengujian latency dari Open VPN.

Tabel 1. Konfigurasi Router *Cisco*

| No | Perintah Pada Router |
|---|---|
| **1** | Router > |
| **2** | Router > enable |
| **3** | Router # configure terminal |
| **4** | Router (config)# interface fastethernet0/0 |
| **5** | Router (config-if)# ip address 192.168.10.1 255.255.255.0 |
| **6** | Router (config-if)# no shutdown |
| **7** | Router (config-if)# exit |
| **8** | Router (config)# interface fastethernet0/1 |
| **9** | Router (config-if)# ip address 10.0.0.1 255.0.0.0 |
| **10** | Router (config-if)# no shutdown |
| **11** | Router (config-if)# exit |
| **12** | Router (config-if)# router rip |
| **13** | Router (config-router)# network 192.168.10.0 |
| **14** | Router (config-router)# network 10.0.0.0 |
| **15** | Router(config-router)# version 2 |
| **16** | Router (config-router)# exit |
| **17** | Router (config)# crypto isakmp policy 10 |
| **18** | Router (config-isakmp)# authentication pre-share |

E-ISSN: 2548-3412; 143-152

| No | Perintah Pada Router |
|---|---|
| **19** | Router (config-isakmp)# hash sha |
| **20** | Router(config-isakmp)# encryption aes 128 |
| **21** | Router (config-isakmp)# group 2 |
| **22** | Router (config-isakmp)# lifetime 86400 |
| **23** | Router (config-isakmp)# exit |
| **24** | Router (config)# crypto isakmp key toor address 10.0.0.0.2 |
| **25** | Router (config-if)# crypto ipsec transform-set TSET es-aes esp-sha-hmac |
| **26** | Router (config-if)# access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168,20.0 0.0.0.255 |
| **27** | Router (config-if)# crypto map CMAP 10 ipsec-isakmp |
| **28** | Router (config-crypto-map)# set peer 10.0.0.2 |
| **29** | Router (config-crypto-map)# match address 101 |
| **30** | Router (config-crypto-map)# set transform-set TSET |
| **31** | Router (config-crypto-map)# Exit |
| **32** | Router (config)# Interface fastethernet0/1 |
| **33** | Router (config-if)# crypto map CMAP |
| **34** | Router # Write |

Sumber: Hasil Penelitian (2020)

Tabel 2. Rincian latency rata-rata pada Open VPN

| Open VPN | | 3des-md5 (ms) | 3des-sha1 (ms) | aes128-md5 (ms) | aes-128-md5 (ms) |
|---|---|---|---|---|---|
| **Ukuran Paket (Byte)** | 100 | 131.574 | 205.325 | 172.573 | 124.463 |
| | 200 | 172.786 | 173.436 | 245.463 | 200.325 |
| | 500 | 141.463 | 638.785 | 351.242 | 189.325 |
| | 1000 | 163.574 | 297.432 | 177.253 | 182.534 |
| | 1500 | 201.232 | 320.434 | 173.326 | 151.967 |
| **Rata-rata(ms)** | | **162.126** | **327.082** | **223.971** | **169.723** |

Sumber: Hasil Penelitian (2020)

Dari tabel tersebut didapat nilai rata-rata dari lima periode pengiriman packet icmp dengan menggunakan service Open VPN. Nilai rata-rata setiap percobaan akan dibandingkan untuk mendapatkan nilay latency kecil diantara kombinasi-kombinasi enkripsi dan otentikasi pada pengujian yang dilakukan.

## 4. Kesimpulan

Setelah melakukan analisis serta uji coba dan simulasi *Virtual Private Network* (VPN), maka dapat disimpulkan sebagai berikut: a). Dari hasil percobaan yang dilakukan menggunakan software *sniffing* wireshark, terbukti OpenVPN Akses Server memberikan keamanan akses data yang baik. b). Fitur *Graphical User Interface(GUI)* berbasis WEB terbukti memberikan kemudahan dalam implementasi baik disisi *server* maupun disisi *client*. Open VPN-Access Server bekerja dengan baik pada saat melakukan koneksi virtual untuk mengakses interkoneksi antar jaringan. Sebaiknya pengujian dilakukan menggunakan beberapa software yang dapat dipergunakan untuk menguji jaringan, selain *software Whiresark*, ada juga s*oftware Putty* untuk digunakan sebagai pengujian jaringan. kita akan mendapatkan perbandingan jika pengujian dilakukan minimal menggunakan 2 (dua) *software* tersebut. Perbandingan tersebut bisa jadi acuan keakurasian keamanan interkoneksi antar perusahaan dengan VPN.

## Referensi

[1] M. Syafrizal, *Pengantar Jaringan Komputer*. Yogyakarta: Andi Offset, 2015.

[2] J. L. Putra, L. Indriyani, and Y. Angraini, “Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna,” *IJCIT (Indonesian J. Comput. Inf. Technol. p-ISSN 2527-449X, e-ISSN 2549-7421*, vol. 3, no. 2, pp. 260–267, 2018.

[3] I. Ruslianto and U. Ristian, “Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura,” *Comput. Eng. Sci. Syst. J.*, vol. 4, no. 1, p. 74, 2019.

[4] R. Toyib and M. Muntahanah, “Pemanfaatan Vpn Dengan Ip Cloud Mikrotik

Menggunakan Jaringan 3G (Studi Kasus : Pt. Bprs Muamalat Harkat Bengkulu)," *Sistemasi*, vol. 8, no. 1, p. 90, 2019.

[5] H. Wijaya, *Belajar Sendiri Cisco ADSL Router, PIX Firewall, dan VPN*. Jakarta: PT. Elex Media Komputindo, 2015.

[6] M. Maryanto, M. Maisyaroh, and B. Santoso, "Metode Internet Protocol Security (IPSec) Dengan Virtual Private Network (VPN) Untuk Komunikasi Data," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 6, no. 2, pp. 179–188, 2018.

[7] C. Widodo, M. Yana, and H. Agung, "Implementasi Topologi Hybrid Untuk Pengoptimalan Aplikasi Edms Pada Project Office Pt Phe Onwj," *J. Tek. Inform.*, vol. 11, no. 1, pp. 19–30, 2018.

[8] K. A. Farly, X. B. N. Najoan, and A. S. M. Lumenta, "Perancangan Dan Implementasi Vpn Server Dengan Menggunakan Protokol Sstp (Secure Socket Tunneling Protocol) Studi Kasus Kampus Universitas Sam Ratulangi," *J. Tek. Inform. Univ. Sam Ratulangi*, vol. 11, no. 1, 2017.

[9] Wagito, *Jaringan Komputer, Teori dan Implementasi Berbasis Linux*. Yogyakarta: Gava Media, 2015.

[10] M. Ryansyah and M. S. Maulana, "Malware Security Menggunakan Filtering Firewall Dengan Metode Port Blocking Pada Mikrotik RB 1100AHx 2," vol. 6, no. 3, pp. 108–112, 2018.

[11] A. Kurniwan, *Network Forensics, Paduan Analisis & Investigasi Paket Data Jaringan Menggunakan Woreshark*. Yogyakarta: Andi Offset, 2018.